## REMARKS

Summary of the Office Action - Status of the claims

Claims 1-22 are pending in the Office Action.

Claims 1-22 are rejected under 35 U.S.C. § 103(a).

Applicants' Response

In this Response, Applicants address the Examiner's rejections. Applicants' silence with regard to the Examiner's rejections of the dependent claims constitutes recognition by the Applicants that the rejections are moot based on Applicants' Remarks relative to the independent claim from which the dependent claims depend. Claims 1-22 are pending. Applicants respectfully traverse all rejections of record.

35 U.S.C. § 103 Rejections

Claims 1-22 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,915,279 to Hogan et al. ("Hogan") in view of U.S. Patent Publication No. 2003/0200184 to Dominguez et al. ("Dominguez").

To reject claims in an application under 35 U.S.C. § 103, an examiner must establish a prima facie case of obviousness. Using the Supreme Court's guidelines enunciated in Graham v. John Deere, 383 U.S. 1, 17 (1966), one determines "obviousness" as follows:

> Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

In *KSR Int'l Co. v. Teleflex Inc.*, the Supreme Court reaffirmed the Graham test, and indicated that although it should not be rigidity applied, a useful test for determining obviousness is to consider whether there is a teaching, suggestion or motivation in the prior art that would

lead one of ordinary skill in the art to combine known elements of the prior art to arrive at the claimed invention. KSR, 82 USPQ2d 1385, 1396 (2007). Importantly, the Court emphasized that a patent Examiner's analysis under § 103 must be made explicit and there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Id.*

Thus, to establish a prima facie case of obviousness, the Examiner has an obligation to construe the scope of the prior art, identify the differences between the claims and the prior art, and determine the level of skill in the pertinent art at the time of the invention. The Examiner must then provide an explicit, cogent reason based on the foregoing why it would be obvious to modify the prior art to arrive at the claimed invention.

Independent Claim 1

Claim 1 recites an issuer platform layer including at least one 3-D Secure authentication program; a merchant plug-in (MPI); an secure payment algorithm (SPA); and a data transport layer, wherein the issuer platform comprises an access control server (ACS) that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value (AAV) and conveys the AAV through the data transport layer to the MPI, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code (MAC).

According to the Examiner, it would have been obvious to a person having ordinary skill in the art to have modified Hogan with the features of Dominguez to arrive at the claimed combination. Applicants traverse, and respectfully request reconsideration.

Dominguez is directed to a payment authentication service that authenticates the identity of a payer during online transactions. A merchant plug-in (MPI) passes a payment authentication request message to the Access control server ("ACS"). *See* Dominguez, Paragraph [0096]. The Access control server requests identity verification, such as a previously-registered password, from the cardholder. *See* Dominguez, Paragraph [0098]. If the identity of the cardholder is successfully identified, the ACS generates a payment authentication response message and sends it to the MPI. *See* Dominguez, Paragraph [0099]. Thus, the message sent to the MPI is for purposes of reporting the results of the authentication process.

Hogan is directed to a secure electronic payment system. When a customer submits an order, data will be transferred from the merchant to the user software using hidden fields in a confirmation page. *See* Hogan, Col. 11 lines 45-58. The user software then sends a request for authentication to the issuer. *See* Hogan, Col. 15, lines 1-8. Authentication data, which may be an Account Holder Authentication Value, is sent in a loop from the issuer to the user software, to the merchant, to the payment organization, and back to the issuer. *See* Hogan, Col. 3 lines 46-50. Hogan explains the purpose of this data:

> The data 420 received by the issuer 406 should be derived from the original authentication data 414, provided that no improper operations have been performed upon authentication data 414 during its trip around the loop. Therefore, the issuer can authenticate the identity of the account holder and verify the authenticity of the transaction based upon the authentication data 414 and the data 420 received from the payment organization 408.

Hogan, Col. 3 lines 50 - 58. Thus, the authentication data is used to authenticate the identity of the account holder.

An example of the AAV is discussed in Cols. 3 and 4. The AAV is a 24 byte data structure, with the bytes assigned as described in Table 1. *See* Hogan, Col. 3 line 59-63. The AAV may include a AAV-Generation Processor Identifier, key identification data, a transaction sequence number, and a message authentication code ("MAC"). *See* Hogan, Table II.

No Motivation to Combine

Applicants submit that claim 1 is patentable over the cited references because one of ordinary skill in the art would have no motivation to combine Dominguez and Hogan. As noted, Dominguez authenticates the identity of the cardholder by requesting information, such as a password, from the cardholder, and then sending a message to the merchant indicating that the identity of the cardholder has been authenticated.

In contrast, Hogan authenticates the identity of the cardholder by sending authentication data (the AAV) to user software. The authentication data, or some portion thereof, is then sent to the merchant, to the payment organization, and back to the issuer. The identity of the issuer is authenticated by ensuring that "no improper operations have been performed upon the authentication data 414 during its trip around the loop." Hogan, Col. 3 lines 52-54. A message indicating that the identity of the cardholder has been authenticated is then sent to the merchant via the payment organization. *See* Hogan, Abstract.

A person having ordinary skill in the art would not modify the authentication method of Dominguez to send the AAV as disclosed in Hogan to the cardholder for authentication purposes because the authentication methods presented in the references are fundamentally different. The authentication method disclosed in Dominguez relies on input from the cardholder, rather than operations performed by each of user software, a merchant, and a payment network, to authenticate the identity of the cardholder. Note that such a combination would also not disclose

every limitation recited in claim 1 because the cardholder would send the AAV right back to the issuer, rather than the AAV being conveyed to the MPI through the data transport layer as required in claim 1.

Further, a person having ordinary skill in the art would not modify the authentication method of Dominguez to send the AAV disclosed in Hogan to the MPI in the payer authentication request response. Hogan discloses that the purpose of the AAV is to authenticate the identity of the cardholder. *See* Hogan, Col. 3 lines 50-58. However, in Dominguez, authentication of the identity of the cardholder is completed before the payer authentication response is generated.

The Combination Does Not Disclose or Suggest Every Limitation of Claim 1

Assuming *arguendo* that one having ordinary skill in the art would have motivation to combine the references, the combination of Dominguez and Hogan still fails to disclose or suggest each and every element recited in claim 1. Dominguez fails to disclose at least an ACS that uses the SPA to generate an AAV, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code.

Hogan does not provide the missing teaching. Hogan fails to disclose or suggest a formatted data structure with a length of at most 20-bytes. Indeed, Hogan describes, "[t]he AAV 802 comprises *24 bytes* of binary data representing 32 Base-64-encoded characters." Hogan, col. 3, lines 62-63, emphasis added. Further, Hogan fails to disclose or suggest that the AAV data structure include bytes that identify the authentication method.

Applicants therefore submit that claim 1 is patentable over the cited references. Independent claim 16 recites similar limitations and therefore is patentable for at least the same reasons as discussed above in relation to claim 1. Dependent claims 2-10 and 17-22, which depend from claims 1 and 16, respectively, are patentable for at least the same reasons. Applicants therefore respectfully request that the rejections be withdrawn and claims 1-10 and 16-22 be allowed.

Independent Claim 11

Independent claim 11 recites a data structure for conveying cardholder transaction authentication information amongst stakeholders in a 3-D Secure Environment, the data structure comprising 20 bytes of Base 64 encoded characters, wherein the first byte is a control byte, bytes 2-9 represent a hash of a merchant name, byte 10 identifies an Access control server (ACS) that authenticates the cardholder transaction by an authentication method, byte 11 identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication Code (MAC), bytes 12 - 15 represent a transaction sequence number identifying a transaction number processed by the ACS, and bytes 16-20 represent the MAC. The Examiner concedes that Hogan fails to disclose such a data structure. However, the Examiner states that Dominguez discloses a data structure as recited in claim 11. *See* Office Action, pp. 6-7. Applicants traverse, and respectfully request reconsideration.

Dominguez is directed towards a method for authenticating the identity of a payer during online transactions. Applicants are unable to identify any data structure disclosed in the reference which discloses the recited elements. Instead, Dominguez only vaguely discusses the Payer Authentication Response message and the Condensed Payer Authentication Response

message, as well as the data fields which may be included therein. *See* Dominguez, Paragraphs [0159] - [0160]; Figs. 10 and 11.

Dominguez fails to disclose a data structure comprising 20 bytes of base 64 encoded characters. Indeed, no data structure of a specific length is mentioned in Dominguez.

Dominguez further fails to disclose a data structure that includes data fields representing a hash of a merchant name, identifying an Access control server (ACS) that authenticates the cardholder transaction by an authentication method, identifying the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication code (MAC), representing a transaction sequence number identifying a transaction number processed by the ACS, or representing the MAC.

The passages identified by the Examiner are not directly relevant. The Abstract provides an overview of the authentication process, but does not disclose or suggest a data structure. Paragraphs [0008] - [0013] comprise the brief summary of the invention. While the condensed payment authentication response message and the payment authentication response message are mentioned in this passage, there is no discussion of the data structure used to communicate such messages.

Hogan does not provide the missing teachings, as discussed above in relation to claim 1.

Applicants therefore respectfully submit that claim 11 is patentable over the cited references. Claims 12-15 depend from claim 11 and are patentable for at least the same reasons. Applicants therefore respectfully request that the rejection be withdrawn and claims 11-15 be allowed.

Dependent Claims 4, 13, and 19

Dependent claim 4 is directed towards a system as recited in claim 1, wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a pair of secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field, and uses the result to populate two bytes of the MAC. Applicants traverse the rejection of claims 4, and respectfully request reconsideration.

Applicants first note that claim 4 depends from claim 1, and therefore is allowable for at least the reasons cited above in relation to claim 1.

Further, Applicants submit that Hogan and Dominguez fail to disclose or suggest each and every limitation of claim 4. Specifically, both Hogan and Dominguez fail to disclose an SPA comprising an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a pair of secret keys. Dominguez does not disclose or suggest a SPA. Hogan discloses that data "is encrypted using *a* secret key…to generate a cryptographic Message Authentication Code (MAC)." Hogan, Col. 6 lines 5-7 (emphasis added). Indeed, Hogan repeatedly refers to the encryption key in the singular. *See* Hogan, Col. 6 lines 27-28 ("Used to identify *the* cryptographic key"); Col. 6 line 61 ("Using *the* key identified by the Key Identification data"); Col. 7 lines 1-2 ("the AAV-verification processor 442 determines *the* secret cryptographic key"). Thus, Hogan fails to disclose or suggest the use of two encryption keys.

Hogan and Dominguez further fail to disclose an encryption algorithm using the pair of secret keys A and B that are identified in the AAV to encrypt a concatenation of the cardholder's account number, card expiration date and service code to generate a three-digit CVC2 field, and using the result to populate two bytes of the MAC. As noted, Dominguez does not disclose or suggest a SPA. Hogan discloses that "[a] CVC2 field which is only available on the signature

panel of [the] card" can be used as a shared secret, for purposes of registration. Hogan, Col. 23 lines 16-17. This CVC2 value is a shared secret, i.e., known by the issuer. *See* Hogan, Col. 22 line 53 -Col. 23 line 21. Further, Hogan fails to disclose use of a card expiration date or a service code in determining the MAC.

Therefore, Applicants submit that claim 4 is patentable over the cited references for these additional reasons. Claims 13 and 19 recite similar limitations. Applicants therefore respectfully request that the rejections be withdrawn and claims 4, 13, and 19 be allowed.

Claims 5, 15, and 20

Claim 5 recites a system as recited in claim 4, wherein the pair of secret keys A and B are 64-bit Data Encryption Standard (DES) keys. Applicants traverse the rejection of claim 5, and respectfully request reconsideration.

Applicants first note that claim 5 depends from claims 1 and 4, and therefore is patentable for at least the reasons discussed above in relation to those claims.

Applicants further submit that Dominguez and Hogan fail to disclose or suggest each and every limitation of claim 5. Indeed, both Dominguez and Hogan fail to disclose a specific type of encryption key, and therefore do not disclose or suggest the use of 64-bit Data Encryption Standard (DES) keys.

Applicants therefore submit that claim 5 is patentable over the cited references for at least these additional reasons. Claims 15 and 20 recite similar limitations. Applicants therefore respectfully request that the rejection be withdrawn, and claims 5, 15, and 20 be allowed.

Claims 10 and 22

Claim 10 recites a system as disclosed in claim 1, wherein the MPI is configured to extract the MAC fields included in a payment authentication response message from the ACS

and to place the extracted MAC in a payment authorization request message to a third party. Applicants traverse the rejection of claim 10, and respectfully request reconsideration.

Applicants first note that claim 10 depends from claim 1, and therefore is allowable for at least the same reasons as discussed above in relation to claim 1.

Applicants further submit that the combination of Dominguez and Hogan fails to disclose each and every limitation of claim 10. As discussed, in Hogan the MAC is sent to the merchant for purposes of authentication, i.e., *before* the identity of the customer has been authenticated. Thus, the MAC is not included in a payment authentication *response* message, as required by claim 4. Indeed, neither Hogan nor Dominguez identify any purpose for the MAC beyond authentication of the identity of a cardholder. Therefore, the MAC would not be included in a message sent subsequent to a payment authentication response message, which is necessarily sent after the identity of the cardholder has been authenticated.

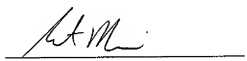
Therefore, Applicants submit that claim 10 is patentable over the cited references for these additional reasons. Claim 22 recites similar limitations. Therefore, Applicants respectfully request that the rejections be withdrawn, and claims 10 and 22 be allowed.

## CONCLUSION

On the basis of the foregoing Remarks, Applicants respectfully submit that the pending claims of the present application are allowable over the cited references. Applicants therefore respectfully request the previous rejections be withdrawn, and that the pending claims be allowed. Favorable consideration and timely allowance of this application are respectfully requested. In the event that the application is not deemed in condition for allowance, the Examiner is invited to contact the undersigned at (212) 408-2538 in an effort to advance the prosecution of this application. If any additional fees are required, please charge Deposit Account No. 02-4377. If any overpayment has been made, please credit Deposit Account No. 02-4377.

February 18, 2010

Respectfully submitted,



Robert L. Maier
PTO Reg. No. 54,291

Eliot D. Williams
PTO Reg. No. 50,822

*Attorney for Applicants*
BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112